Allen-Bradley® Stratix 5900™ Services Router

The Stratix 5900 Services Router, catalog number 1783-SRKIT, combines a number of modern security functions into a single appliance to help protect your Industrial Automation and Control Systems network, not only at the perimeter, but also as the cell/zone level. The compact and robust Stratix 5900 Services Router is an industrially hardened, managed router that also provides a number of managed switching features. The Stratix 5900 can help simplify the network infrastructure and machine integration by providing a single device to implement VPN, Firewall, NAT, and many other services. It helps provide a rapidly deployable, reliable and secure solution designed specifically for industrial applications.

These capabilities make the services router well suited for:

- **Site-to-Site Connection** – establishes encrypted tunnels between trusted remote Industrial Zones over an untrusted network using a site-to-site VPN connection
- **Cell/Area Zone Firewall** – protects Cell/Area Zone from the greater Industrial Zone by limiting the flow of information and access
- **OEM Integration** – allows OEM providers to define the flow of information and access to their machine from the greater network while making use of features such as NAT

**Features**

- Fully integrated with Cisco IOS, the Stratix 5900 uses a wide area network (WAN) port and four additional Ethernet-ports to help deliver:
  - Highly secure real-time control communication
  - Secure routing and firewall capabilities
  - Virtual Private Network (VPN)
  - Intrusion protection capabilities
  - Network Address Translation (NAT)
  - NBAR protocol filtering
  - Access Control Lists (ACL)
  - Quality of Service (QoS) for prioritization

**Additional features ideal of industrial applications include:**
- Extended shock and vibration capability
- DIN rail mount
- A temperature range of minus 25 C to 60 C

**Configure, Monitor and Maintain**

- **Stratix 5900 Device Manager**
  - Web-based graphical device management tool
  - Manage and diagnose network issues
  - Alarm tools to alert, identify and help solve network problems

- **Stratix Configurator**
  - PC-based application software for device management of IOS-based Stratix products
  - Easy-to-use configuration wizards for router, firewall, intrusion prevention system (IPS), VPN, unified communications, WAN and LAN configurations

- **Cisco Command Line Interface (CLI)**
Applying the Stratix 5900 Services Router

The control system is no longer an isolated operation. As industrial organizations move towards greater visibility into their operations and advanced analytics, the need to establish a seamless flow of information from device to enterprise becomes extremely important. An increased need for data gathering within the factory, and connectivity from device to DMZ to remote industrial sites, from manufacturing zone to manufacturing zone, all have become a requirement of modern industrial networks. With this trend towards the connected enterprise, you now not only have to create a capable and reliable architecture, but a secure one as well. With the Stratix 5900 Services Router, you can help protect and secure your industrial control system.

The Stratix 5900 Services Router enables manufacturing locations to connect to and communicate with remote outstations. A remotely located machine that needs to securely talk to a plant-based machine can now do so using the VPN and firewall features of the device.

This is a common application for industries where equipment that is dispersed across vast distances needs to communicate with each other over an untrusted network to operate a common process.

The appliance allows areas or machines within a factory to be isolated from each other. Using a services router with firewall capabilities allows you to monitor and block an input, output or system call that does not meet the firewall’s configured policy. When combined, a VPN and firewall create a more robust, more secure network.VPNs can also help create a secure tunnel for server-machine communications to protect the transfer of important data from other machines in the facility.

By creating this segmentation, you are able to harden your network infrastructure so only the right people and/or equipment can communicate with critical production processes and reduce the risks from intentional or unintentional tampering.

www.rockwellautomation.com